§ 748.2 Bank Secrecy Act compliance programs and procedures.

(a) *Purpose*. This section is issued to ensure that all federally-insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance with the requirements of subchapter II of chapter 53 of title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act, and the implementing regulations promulgated thereunder by the Department of Treasury, 31 CFR part 103.

(b) *Compliance Procedures*. On or before August 1, 1987, each federally-insured credit union shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with recordkeeping and reporting requirements set forth in subchapter II of chapter 53 of title 31, United States Code, the Financial Recordkeeping and Reporting of Currency and Foreign Transactions Act and the implementing regulations promulgated thereunder by the Department of Treasury, 31 CFR part 103. This program shall be reduced to writing, approved by the board of directors of the institution, and noted in the minutes.

(c) *Contents of compliance program*. Such compliance program shall at a minimum—

(1) Provide for a system of internal controls to assure ongoing compliance;

(2) Provide for independent testing for compliance to be conducted by credit union personnel or outside parties;

(3) Designate an individual responsible for coordinating and monitoring day-to-day compliance; and

(4) Provide training for appropriate personnel.

(Approved by the Office of Management and Budget under control number 3133–0094)

[52 FR 2861, Jan. 27, 1987, as amended at 52 FR 8062, Mar. 16, 1987]

APPENDIX A TO PART 748—GUIDELINES FOR SAFEGUARDING MEMBER INFORMATION

TABLE OF CONTENTS

I. INTRODUCTION

The Guidelines for Safeguarding Member Information (Guidelines) set forth standards pursuant to sections 501 and 505(b), codified at 15 U.S.C. 6801 and 6805(b), of the Gramm-Leach-Bliley Act. These Guidelines provide guidance standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of member information.

A. *Scope*. The Guidelines apply to member information maintained by or on behalf of federally-insured credit unions. Such entities are referred to in this appendix as ''the credit union.''

B. *Definitions*. 1. *In general*. Except as modified in the Guidelines or unless the context otherwise requires, the terms used in these Guidelines have the same meanings as set forth in 12 CFR part 716.

2. For purposes of the Guidelines, the following definitions apply:

a. *Member* means any member of the credit union as defined in 12 CFR 716.3(n).

b. *Member information* means any records containing nonpublic personal information, as defined in 12 CFR 716.3(q), about a member, whether in paper, electronic, or other form, that is maintained by or on behalf of the credit union.

c. *Member information system* means any method used to access, collect, store, use, transmit, protect, or dispose of member information.

d. *Service provider* means any person or entity that maintains, processes, or otherwise is permitted access to member information through its provision of services directly to the credit union.

II. STANDARDS FOR SAFEGUARDING MEMBER INFORMATION

A. *Information Security Program*. A comprehensive written information security program includes administrative, technical, and physical safeguards appropriate to the size and complexity of the credit union and the nature and scope of its activities. While all parts of the credit union are not required to

implement a uniform set of policies, all elements of the information security program must be coordinated.

B. *Objectives.* A credit union's information security program should be designed to: ensure the security and confidentiality of member information; protect against any anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member. Protecting confidentiality includes honoring members' requests to opt out of disclosures to nonaffiliated third parties, as described in 12 CFR 716.1(a)(3).

III. DEVELOPMENT AND IMPLEMENTATION OF MEMBER INFORMATION SECURITY PROGRAM

A. *Involve the Board of Directors.* The board of directors or an appropriate committee of the board of each credit union should:

1. Approve the credit union's written information security policy and program; and

2. Oversee the development, implementation, and maintenance of the credit union's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. *Assess Risk.* Each credit union should:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of member information; and

3. Assess the sufficiency of policies, procedures, member information systems, and other arrangements in place to control risks.

C. *Manage and Control Risk.* Each credit union should:

1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the credit union's activities. Each credit union must consider whether the following security measures are appropriate for the credit union and, if so, adopt those measures the credit union concludes are appropriate:

a. Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

b. Access restrictions at physical locations containing member information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

c. Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

d. Procedures designed to ensure that member information system modifications are consistent with the credit union's information security program;

e. Dual controls procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to member information;

f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into member information systems;

g. Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; and

h. Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technical failures.

2. Train staff to implement the credit union's information security program.

3. Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.

D. *Oversee Service Provider Arrangements.* Each credit union should:

1. Exercise appropriate due diligence in selecting its service providers;

2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and

3. Where indicated by the credit union's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a credit union should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. *Adjust the Program.* Each credit union should monitor, evaluate, and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its member information, internal or external threats to information, and the credit union's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to member information systems.

F. *Report to the Board.* Each credit union should report to its board or an appropriate committee of the board at least annually.

This report should describe the overall status of the information security program and the credit union's compliance with these guidelines. The report should discuss material matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. *Implement the Standards.*

1. *Effective date.* Each credit union must implement an information security program pursuant to the objectives of these Guidelines by July 1, 2001.

2. *Two-year grandfathering of agreements with service providers.* Until July 1, 2003, a contract that a credit union has entered into with a service provider to perform services for it or functions on its behalf satisfies the provisions of paragraph III.D., even if the contract does not include a requirement that the servicer maintain the security and confidentiality of member information, as long as the credit union entered into the contract on or before March 1, 2001.

[66 FR 8161, Jan. 30, 2001]

PART 749—RECORDS PRESERVATION PROGRAM AND RECORD RETENTION APPENDIX

Sec.

AUTHORITY: 12 U.S.C. 1766, 1783 and 1789, 15 U.S.C. 7001(d).

SOURCE: 66 FR 40579, Aug. 3, 2001, unless otherwise noted.

§ 749.0 What is covered in this part?

This part describes the obligations of all federally insured credit unions to maintain a records preservation program to identify, store and reconstruct vital records in the event that the credit union's records are destroyed. It establishes flexibility in the format credit unions may use for maintaining writings, records or information required by other NCUA regulations. The appendix also provides guidance concerning the appropriate length of time credit unions should retain various types of operational records.

§ 749.1 What are vital records?

Vital records include at least the following records, as of the most recent month-end:

(a) A list of share, deposit, and loan balances for each member's account which:

(1) Shows each balance individually identified by a name or number;

(2) Lists multiple loans of one account separately; and

(3) Contains information sufficient to enable the credit union to locate each member, such as address and telephone number, unless the board of directors determines that the information is readily available from another source.

(b) A financial report, which lists all of the credit union's asset and liability accounts and bank reconcilements.

(c) A list of the credit union's financial institutions, insurance policies, and investments. This information may be marked ''permanent'' and stored separately, to be updated only when changes are made.

§ 749.2 What must a credit union do with vital records?

The board of directors of a credit union is responsible for establishing a vital records preservation program within 6 months after its insurance certificate is issued. The vital records preservation program must contain procedures for storing duplicate vital records at a vital records center and must designate the staff member responsible for carrying out the vital records duties. Records must be stored every 3 months, within 30 days after the end of the 3-month period. Previously stored records may be destroyed when the current records are stored. The credit union must also maintain a records preservation log showing what records were stored, where the records were stored, when the records were stored, and who sent the records for storage. Credit unions, which have some or all of their records